Consortium Blockchain-Based Student Status Management Framework

Jinxi Yang, Jianmao Xiao(✉), Jiangyu Wang, Yujie Liu, Wei Yang, Zuoyi Liao, and Qiangqiang Zhou

School of Software, Jiangxi Normal University, Nanchang 330027, China
{jm_xiao,yw,qiang}@jxnu.edu.cn

Abstract. Student status management has always been an indispensable part of the education system, but due to the insufficient application of information technology, there are still a series of pain points in the traditional student status management system, such as easy to falsify student status, serious information islanding, and complex management. Blockchain 3.0 is a consortium blockchain model that uses protocols and consensus mechanisms for property rights confirmation, measurement and storage, with the characteristics of decentralization, immutability, traceability, collective maintenance, security and reliability, etc., which puts forward excellent solutions for student status management. This paper uses the thinking mode and framework of the blockchain to improve the logic and storage mode of the previous student status management system, and uses the Fabric consortium blockchain framework to design and realize a student status management system that can be initially put into use. Test results show that the throughput of the student status chain system can be stabilized at 200tps, which can basically meet the actual application needs of the student status management system.

Keywords: Blockchain · Student status management · Smart contract · Education · Consortium Blockchain

1 Introduction

Student status is a symbol of determining the identity of students, which is closely related to students' right to education, and is also used as an important basis for the certification of social talents, which continues to receive widespread attention from all walks of life [1,2]. Within colleges and universities, student status management needs efficient, convenient and safe management system support. At the social level, student status certification is an important evaluation criterion for employers to evaluate talents, which needs true, reliable and rich talent education background data information. As an integral part of the operation of society, the student registration system still has a lot of room for demand and the need to build a solid foundation.

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2023
Published by Springer Nature Switzerland AG 2023. All Rights Reserved
Y. Cao and X. Shao (Eds.): MONAMI 2022, LNICST 474, pp. 18–31, 2023.
https://doi.org/10.1007/978-3-031-32443-7_2

At the level of student status management, most schools in China currently rely on the student information network, and some schools use their own independent student status management system. In this management model, many problems have cropped up, such as mading irreparable mistakes in student status because of the management negligence, which eventually leads to students being unable to graduate normally, been compromised and attacked on account of database intrusions, resulting in the collapse of the student status management system and malicious tampering of data, and high load on the student status management system during the opening and graduation seasons give rise to system congestion. These problems have hindered the functioning of society and need to be addressed urgently [2].

When conducting academic certification, in addition to referring to CHSI, most companies often spend a lot of money and time to entrust back-adjustment companies to find out the authenticity of personal information, which reflects the current problem that the academic certification body is still not enough to win enough trust. Therefore, it is also important to create a student certification platform that can build a high level of trust in society. As an emerging data management method with decentralization, transparency, security and strong confidentiality, blockchain technology has pointed out a new path for student status management [3] Zhong-Zhen Li et al. [4] have already proposed the idea of using blockchain technology for student status management in 2019, this work mainly uses the consortium blockchain smart contract technology and blockchain storage method to manage and store the student status, this paper improves on this basis, deepens the advantages of the smart contract using the blockchain, improves the closedness of the student status management, and introduces and designs a student status management depository framework based on the consortium blockchain, which can be used to help solve a series of problems such as poor sharing of student status information between universities, excessive reliance on third-party authoritative institutions for information credibility, excessive data storage, inconsistent award recognition, and low information security. The main features of the framework are as follows: by linking universities within the alliance chain, the problem of information islands between multiple universities is solved, and the migration of student registrations between schools is facilitated. In addition, the using of the blockchains mart contract scheme can quickly generates the student status early warning scheme, and in the form of deploying smart contracts within the organizational nodes established by each university, uses the consensus mechanism [5] to reach an award consensus among the universities. The contributions of this paper are as follows:

- We proposed the student status management and storage model under the framework of blockchain, providing a brand new solution for the pain point of the traditional student status information management and storage.
- We deepened the application scope and thinking of smart contract, analyzes the network and storage architecture of Fabric, and broadens the application approach of blockchain.

– We tested the performance of the system under normal running state and analyzed the change of system throughput with nodes.

2 Related Work

2.1 Blockchain

Blockchain technology is a collection of distributed ledgers, cryptography, consensus algorithms and a series of technologies [6], first has been known as the core technology of the Bitcoin system, although mining and speculation and other behaviors violate the core values of society, resulting in a large waste of resources, but the blockchain technology has entered the 3.0 era as a great innovation, and successfully "out of the circle" [7]. It has put forward new challenges and opportunities for all walks of life, and China has also proposed a large number of incentives for the development of blockchain. At present, many domestic and foreign research has made great progress in the application of blockchain, for example, Abeyratne et al. [8] proposes to use blockchain to provide a highly trusted, transparent, collectively maintained ledger for the supply chain information platform, and provide traceability for it. Christidis K et al. [9] combines blockchain with the Internet of Things to achieve service sharing through the core concept of P2P. Hou H et al. [10] proposed that blockchain combines e-government to increase information sharing and transparency. Moreover, many ideas and researches have emerged on the cross-application of blockchain transactions, blockchain currency, blockchain insurance, blockchain news verification and other fields [11].

2.2 Blockchain Education

The transparency of the blockchain system and the immutable data are fully applicable to the credit management of students, further education and employment, academics, qualification certificates, industry-university cooperation, etc., and have important value for the healthy development of education and employment. The application of blockchain education has been carried out in many countries for a long time: Kazakhstan built a blockchain kindergarten platform to reduce the opacity of kindergarten information and provide more objective choices for parents. South Korea's Pohang University of Science and Technology led the development of blockchain knowledge sharing platform to break down communication barriers between schools. MIT MediaLLab issued blockchain certificates to more than 100 students, ensuring that the pilot student's student status was immutable [12]. On the basis of foreign research results, a series of studies on blockchain student status have been carried out in China [13]. The current domestic existing a lot of research about student status block chain, By indexing CNKI with student status and blockchain as keywords, we found that there were 21 related papers published in the past 18 to 22 years, but most of the research stayed at the level of feasibility analysis and theoretical research,

and most of the research only focused on the decentralization and security of the blockchain, and did not use the blockchain system to make landmark innovations in the logic and form of student status management, nor did it actually consider the development details and specific needs. Therefore, this paper uses the technology of the consortium blockchain, builded a blockchain platform for the union of universities, through the adjustment of the consensus mechanism and the use mode of smart contracts, establish a consensus on awards and mutual recognition of student status among universities [14].

3 Overall Architecture and System Implementation

This paper is based on Fabric's school registration system framework logic as shown in the Fig. 1.

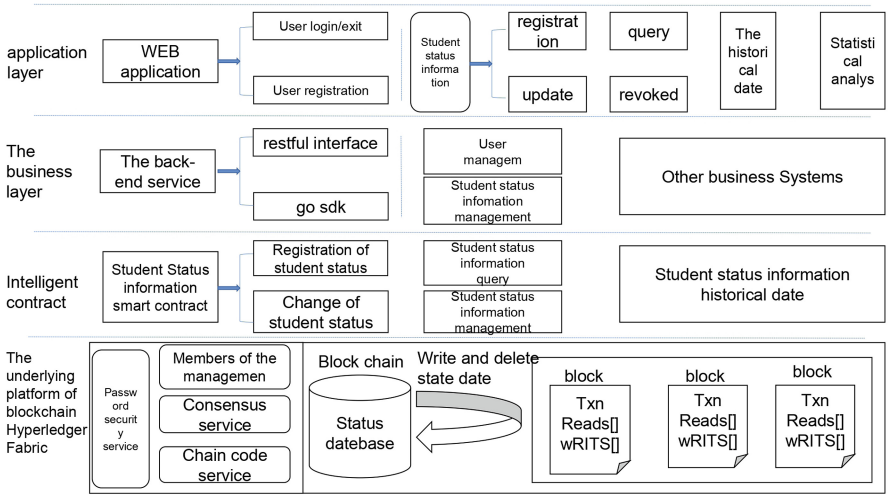

Fig. 1. system framework

The overall system architecture can be divided into surface layer and bottom layer according to the depth. The surface layer is composed of application layer, service layer and smart contract, and the bottom layer is supported by fabric network and storage technology.

3.1 Surface Frame

Application Layer. The application layer mainly includes the user's registration login, the tracing query of the student's educational background information, the administrator's query and management of the student's information, which is edited by the JavaScript and Vue framework to realize the interactive page, deployed on the server by using the Nginx technology, and provides the operating interface of the information in the chain to the vast nodes.

Business Layer. As the front-end and back-end interaction service, the service layer transfers the parameters to the web end by calling the Restful interface, realizes the interaction with the blockchain bottom layer including the smart contract through Fabric-Go-SDK, and calls the invoke function in the smart contract to operate the data. When the system is in operation, the front end will pass in parameters and request to call the smart contract. When the rules of the smart contract are effective, the data will be transmitted to the bottom layer for processing.

Contract Layer. The smart contract layer is the key technology of the alliance chain and the core innovation of the blockchain student status system [15]. The smart contract layer has two functions: award mutual recognition and student status early warning. The principle of award mutual recognition is based on the consensus rule of smart contract. The Education Bureau forms the classification of awards after the recognition of smart contract by issuing awards in the chain, which to a certain extent opens up the barriers to the talent comparison between different schools and prevents some malicious fraud of awards. The student status early warning function issues student status early warning rules to students of all grades of the school through the school node to automatically realize the student status early warning judgment.

3.2 Bottom Frame

The bottom layer of student status chain is composed of Fabric bottom network architecture kernel and blockchain with CouchDB database storage [16]. The network architecture and storage logic inside the school log chain is the core of the whole system. The school log chain network layer is mainly responsible for the endorsement of the school administrator node users, the operation of the consensus service, the chain code service and the encryption service. HSM is used to provide advanced protection for the digital key. Node discovery and data broadcasting are realized through Gossip, node communication is realized through channel, and the application function is realized through the interaction between the service layer and the application layer. At the same time, the CouchDB database directly supported by Fabric is connected inside and outside the student status chain to store huge student data, and the student data contained in the ledger is saved to the database with faster speed in a similar way to the merkle tree storage. Meanwhile, the high support of CouchDB for rich query is utilized to efficiently use the database storage space and enhance the query efficiency of data.

Network Architecture. The network architecture of the student status chain mainly includes a client node for interaction between the school node user and the

student status chain, a CA node for verifying identity information, a Peer node for processing smart contracts, maintaining student information, and processing student requests and responses, and an Orederer node for receiving, packaging, sorting and generating student status information blocks and broadcasting [17]. Nodes communicate with each other through channels to ensure data security. The network architecture model of student status chain node as shown in the Fig. 2.

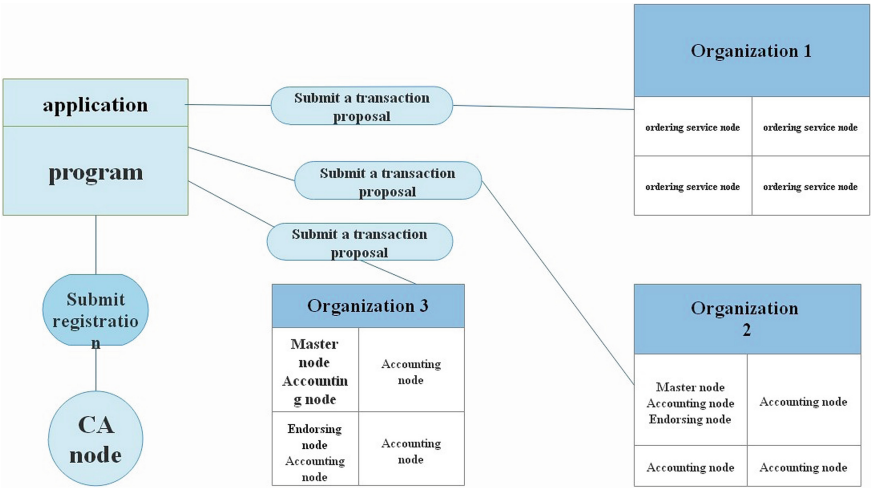

Fig. 2. Network architect

As the division of labor of nodes is clear, so it is different from the public chain. The alliance chain is a weak centralization rather than a decentralized framework, which is a double-edged sword for the application of blockchain, but it has a good coupling with the school status management. The student status chain uses the Kafka protocol to build a conventional fabric network architecture [16]. After the user sends a change or query request to the student status information at the front end, the user sends the modification action to the CA node through the client node for authorization. After the CA node authorizes and issues the self-signed root certificate of the node, the Endors endorsement node stores the operation in the node in the form of "transaction information". Only the endorsed student status information can be submitted and added to the alliance chain. After the endorsement is completed, the Orderer node sorts the endorsed information by consensus, packages the block and broadcasts. The student status information is recorded by each peer node through Gossip protocol, and each node updates the world status tree and node information. The Node network information transmission logic as shown in the Fig. 3.

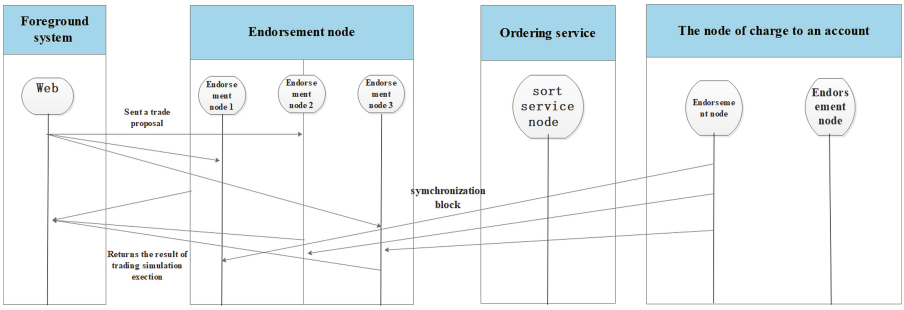

Fig. 3. Node network information transmission logic

Storage Schema. The data structure of student status chain is composed of block header and block body. The block header stores the basic information of the block. The block body stores the transaction and storage data in the block. The hash value of the previous block is used to form a unique link to locate the next block, which is connected to form a block chain [18]. The deep and huge other data is stored in the state database of the alliance chain in the form of key value pairs. It is worth mentioning that in order to realize the time traceability and anti-tamper mechanism of data in public chains such as Bitcoin, the state of data will not be saved in the blockchain, only the change of data will be saved. In order to solve the fatal problem of data query difficulty in traditional blockchain, Hyperledger Fabric the concept of "world state" is introduced. When a record is saved in the block, the world state of the corresponding Key will be updated synchronously. When a key value needs to be queried, you only need to query the corresponding world state without full-chain traversal [19]. The concept of world state greatly reduces the query overhead of blockchain, makes a revolutionary contribution to blockchain enterprise, and also plays an important role in this work.

The data stored in the blockchain includes "ledger" number, "ledger" data, block index, world tree status and historical data. The "ledger" is used to store student information and the modification of student information, so as to organically combine the blockchain and student status storage. In the blockchain application of the system, we use the classic hierarchical storage mode, and the data is stored in the blockchain and CouchDB database hierarchically by type. On the blockchain, the saved work is completed by the Peer node, which maintains four databases, i.e. IdStore, StateDB, HistoryDB and BlockIndex, which are indispensable key information in the chain. The vast student database is stored in the built-in database CouchDB. The storage system architecture as shown in the Fig. 4.

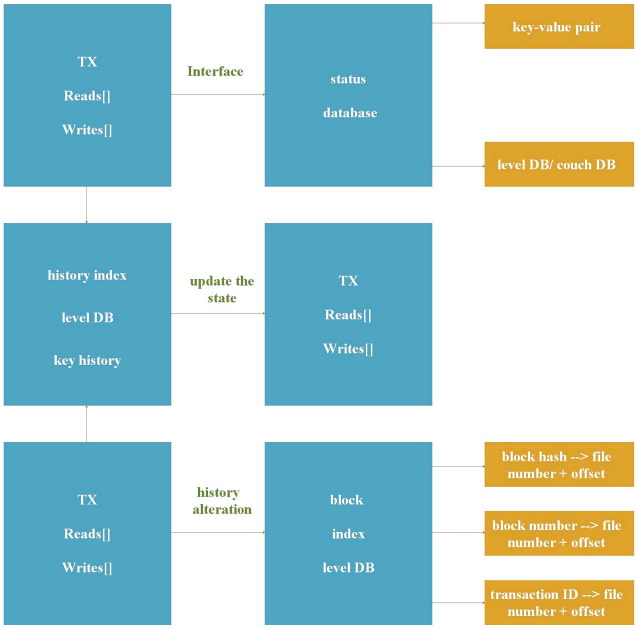

Fig. 4. storage system architecture

The "ledger" is used to store students' information and the modification of students' information. It is stored in the CouchDB database together with the historical status index and the block index. As for these data, it inevitably involves students' personal privacy. Therefore, this paper proposes to use SHA256 encryption algorithm [20] to encrypt students' data in one direction. Overall, SHA256 is similar to the operation flow of hash functions such as MD4, MD5, and HSA-1. Before the message to be hashed continues the hash calculation, the following two steps shall be performed:

- Complements the private information of students so that the final length is a multiple of 512 bits.
- Block messages in 512-bit units.

$$M_1, M_2, M_3, M_4, \cdots, M_n \tag{1}$$

The student private information blocks will be processed one by one: starting with a fixed initial hash H_0, the following sequence is calculated:

$$H_i = H_{i-1} + c^{M_i}(H_{i-1}) \tag{2}$$

where C is the compression function of SHA256, the plus sign is mod 2^{32}'s addition. By using the flexibility of SHA256 algorithm's input length and using SHA256 one-way encryption to protect the students' partial information, the privacy of partial information is strengthened. When the students

need to verify this part of information to others, they need to input Plaintext, and then use the encryption algorithm for one-way encryption to compare with the Ciphertext saved in the database, and the information authenticity can be proved by successful comparison.

4 Analysis of Experimental Results

Performance Test. Blockchain technology is gaining attention, but it is not possible to test the performance of the various blockchain platforms available before creating solutions to business problems. To address this pain point, the Hyperledger community provides a tool called Hyperledger Caliper that can be used to test the performance of blockchain platforms [21]. Caliper is a blockchain benchmark framework that allows users to measure the performance of a particular blockchain implementation using a predefined set of use cases. Caliper will generate reports with many performance metrics, such as TPS (transactions per second), transaction latency, resource utilization, and so on. The goal is to use Caliper results as a reference to support the selection of a suitable blockchain implementation. User-specific use cases. Given the diversity of blockchain configurations, network setups, and specific use cases, it is not intended as an authoritative performance assessment, nor is it for simple comparison purposes. The caliper's running logic as shown in the Fig. 5.

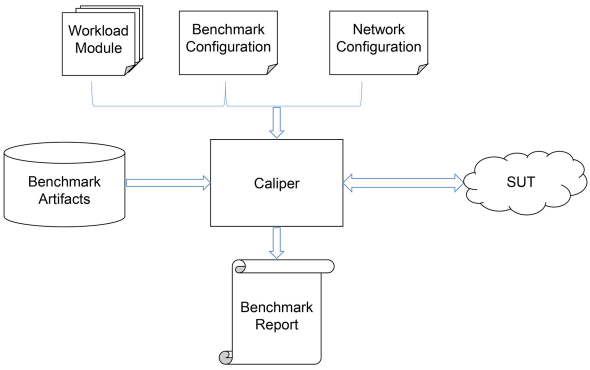

Fig. 5. Caliper's running logic

4.1 System Test Environment

In order to test system performance by ciliper, the author of this article set up the test environment and began rigorous testing. The test environment as shown in Table 1.

Table 1. Test Environment

node deploym	Versi
Operating system	Ubantu 20.04.3
CPU	Interl code i7
Memory	16G DDR4
Hard disk	1T HDD
Hyperledger Fabric	2.2.0
Docker	20.03

4.2 System Test Cases and Results

System Test. For different types of universities and degrees, the test case collected the information of 50 students from 10 universities. Due to space reasons, here to Jiangxi Normal University students as an example to operate.The test example as shown in Fig. 6.

```
'use strict';

const { WorkloadModuleBase } = require('@hyperledger/caliper-core');
class MarblesInitWorkload extends WorkloadModuleBase {
    constructor() {
        super();
        this.txIndex = -1;
        this.entityID=['360202020202020200','360202020202020201','360202020202020202','360202020202020203','360202020202020204'];
        this.name = ['Xiaolin Cheng','Yuyu liu','Liwei  Liu','Qiqi Hua','ZengHao'];
        this.birthday = ['2002-11-7','2002-10-3','2001-1-7','2000-9-7','2002-7-7'];
        this.age = ['19','20','21'];
        this.place = ['JiuJiang','JDZ','NC','JiuJiang','ShangRao'];
        this.nation = ['The han nationality','The han nationality','miao'];
        this.address = ['JDZ','NC','JDZ'];
        this.sex = ['male','male','female'];
        this.id = ['20202610','20202611','20202612'];
        this.states = ['1','1','1'];
        this.schoolName = ['Jiangxi Normal University','Jiangxi Normal University','Jiangxi Normal University'];
        this.enterTime = ['2020-9-12','2020-9-12','2020-9-12'];
        this.graduateTime = ['2024-6-24','2024-6-24','2024-6-24'];
        this.major = ['Computer Science and Technology','Computer Science and Technology','Computer Science and Technology'];
        this.grade = ['1','2','1'];
        this.credit = ['20','40','60'];
        this.averageScore = ['79','79','79'];
        this.poorsubsid = ['0','0','0'];
        this.aSW = ['0','0','0'];
        this.level = ['Undergraduate course','Undergraduate course','Undergraduate course'];
    }
```

Fig. 6. Test case

Test Results. This paper mainly tested open, Query, transfer and other methods. From the figure, we can clearly see the success rate of the project, transaction throughput, transaction delay (minimum, maximum, average, percentage), resource consumption (CPU, memory, network IO, etc.), and open, The success rate of query method is almost 100%, and the highest success rate of Test test is 32.90 TPS. Detailed test results as shown in Table 2.

Table 2. Test results about throughput

Test	Name	Succ	Fail	Send Rate	Max latency	Min latency	Avg latency	Throughput
1	open	100	0	48.8tps	4.88s	3.65s	4.11s	17.4tps
2	query	100	0	56.8tps	1.99s	0.12s	1.44s	32.9tps
3	transfer	33	66	50.8tps	5.42s	2.41s	5.02s	5.11tps

This article is mainly on the docker environment, in this environment, there are two groups: each group contains a peer node(Peer0.org1.example.com and Peer0.org2.example.com), a special deposit certificate of the ca nodes, There are CouchDB nodes to enhance security for compliance and data protection in the blockchain, as well as an organization node. It is not difficult to find the memory occupied by nodes in the figure. Peer nodes account for most of the memory, so the CPU utilization is also very high. Blockchain network consists of peer nodes, each of which can save a copy of ledger and a copy of smart contract. Therefore, the input and output of transactions are mainly dominated by peer nodes. Detailed test results as shown in Table 3.

Table 3. Test results about the use of organization

NAME	Memory	CPU	Traffic in	Traffic Out	Disc Out	Disc write
Peer0.org1.example.com	264.4MB	9.54%	717.6KB	468.7KB	536.0KB	704.0KB
Peer0.org2.example.com	266.4MB	9.73%	719.1KB	512.2KB	860.0KB	704.0KB
Ca.org1.example.com	15.5MB	0.00%	0KB	0KB	0KB	0KB
Couchdb.org1.example.com	90.5MB	8.49%	181.5KB	297.7KB	296.0KB	260.0KB
Ca.org2.example.com	7.9MB	0.00%	0KB	0KB	0KB	0KB
Couchdb.org2.example.com	92.9MB	7.00%	301.7KB	301.7KB	156.0KB	272.0KB
Order.example.com	31.9MB	2.35%	819.1KB	819.1KB	548.0KB	508.0KB

System throughput refers to the number of transactions that a system can process per unit time, which is an important indicator used to measure system performance. For online trading systems, system throughput refers to the number of transaction requests successfully processed and responded to per unit of time. Calculation of average number of concurrent users:

$$C = nL/T \tag{3}$$

where C is the average number of concurrent users, N is the average number of daily access users, L is the average time between login and logout (average operation time) in a day, and T is the length of time. When there is no performance bottleneck, there is a certain correlation between throughput and virtual users, which can be calculated by the following formula:

$$F = VU * R/T \tag{4}$$

F is throughput, VU is the number of virtual users, R is the number of requests sent by each virtual user, and T is the time taken for the performance test. In the case of RAFT algorithm, the throughput of the student roll chain system can be stable at 200tps and it has the commercial function of carrying the student roll storage system. It can be seen that the read throughput decreases while the write throughput increases with the increase of the number of nodes. The read throughput and the write throughput as shown in Fig. 7.

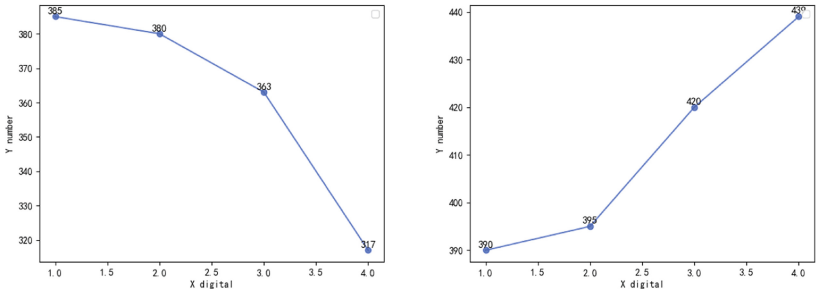

Fig. 7. Experimental results of the authors

5 Conclusion

The use of blockchain technology has slowly shifted from the traditional financial industry to all walks of life in society, this paper combines blockchain technology, in view of the traditional student registration management certificate system information islands, management complexity, user security, storage transience and other pain points, proposes a new type of multi-organization joint student status chain management and registration system, which effectively combines schools, academic affairs offices, and employers, and develops a Hyperledger Fabric consortium blockchain system [22] with basic functions. The test analysis shows that the system has higher throughput compared with other similar blockchain systems, and has stronger security and sharing compared with the traditional student status management system. However, the system proposed in this paper still has throughput and other aspects' problems to be improved in system security. With the further solution of the problems, blockchain will play

a greater role in the field of education. In the future, enterprises can be continuously introduced into the Consortium blockchain, and external certification of academic qualifications can be completed in the system through the cooperation of schools, enterprises and the Ministry of Education, so as to further expand the application of this framework.

Acknowledgements. This work is supported by the No. 62067003, 62262030, National Natural Science Foundation of China (NSFC) under Grant No. 61962026, the National Natural Science Key Foundation of China grant No. 61832014 and No. 62032016, the National Natural Science Foundation of China under Grant No.62002143, the Natural Science Foundation of Jiangxi Province under Grant No. 20192ACBL21031 and the Foundation of Jiangxi Educational Committee under Grant No. GJJ210338.

References

1. Cheng, Y.: Legal theory discussion on several issues of college dropout right - legal theory analysis on the first case of diploma dispute caused by college dropout in china. Law (04), 56–61 (2000)
2. Lin, W.: Practice and thinking of educational administration informationization in colleges and universities. Shenzhou (1), 1 (2018)
3. Geng, F., Lin, C.: Blockchain technology: an emerging technology driving education revolution. Chin. Med. Educ. Technol. **31**(6), 5 (2017)
4. Li, Z., Gao, C., Min, L., Dai, C., Yi, F.: School roll management system based on blockchain technology. J. Sichuan Univ. Nat. Sci. Ed. **56**(3), 7 (2019)
5. Yang, Y., Zhang, S.: Overview of blockchain consensus mechanism. Inf. Secur. Res. **4**(4), 11 (2018)
6. Cheng, S., Shi, W., Liu, L.: Overview of blockchain technology (2016)
7. Yong, Y., Wang, F.Y.: Development status and prospect of blockchain technology. Zidonghua Xuebao/Acta Automatica Sinica **42**(4), 481–494 (2016)
8. Abeyratne, S.A., Monfared, R.: Blockchain ready manufacturing supply chain using distributed ledger (2016)
9. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. IEEE Access **4**, 2292–2303 (2016)
10. Hou, H., Pan, Q.: Research of it outsourcing strategy and evaluation systems in China. In: 2011 International Conference on Computer Science and Service System (CSSS) (2011)
11. Marc, P.: Blockchain technology: Principles and applications. Post-Print (2016)
12. Wu, Y., Cheng, G., Chen, Y., Wang, X., Ma, X.: Research status, hot spot analysis and development thinking of "blockchain + education" at home and abroad. Distance Educ. J. **38**(1), 12 (2020)
13. Li, Q., Zhang, X.: Blockchain: using technology to promote openness and credibility in education. Distance Educ. J. **35**(1), 9 (2017)
14. Huang, S.L., Shen, D.Q., Liang, W., Huang, R.J.: Study on the adaptability of college student status management and information management system. China Manag. Informationization **19**(10), 173–174 (2016)
15. Lauslahti, K., Mattila, J., Seppl, T.: Smart contracts - how will blockchain technology affect contractual practices? ETLA Reports (57) (2017)
16. Nguyen, M.Q., Loghin, D., Dinh, T.: Understanding the scalability of hyperledger fabric. arXiv preprint arXiv:2107.09886 (2021)

17. Leng, J., Lu, X., Jiang, Y., Li, G.: A survey of research on consortium chain consensus mechanism. Data Anal. Knowl. Discov. **5**(1), 10 (2021)
18. Dinh, T., Liu, R., Zhang, M., Chen, G., Ooi, B.C., Wang, J.: Untangling blockchain: a data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. **30**(7), 1366–1385 (2017)
19. Chen, Y., Chen, S., Liang, J., Feagan, L.W., Han, W., Huang, S., Wang, X.S.: Decentralized data access control over consortium blockchains. Inf. Syst. **94**, 101590 (2020)
20. Appel, A.W.: Verification of a cryptographic primitive: SHA-256. ACM SIGPLAN Notices **50**(6), 153–164 (2015)
21. Mazzoni, M., Corradi, A., Nicola, V.D.: Performance evaluation of permissioned blockchains for financial applications: the consensys quorum case study. Blockchain Res. Appl. **3**(1), 12 (2022)
22. Androulaki, E., Manevich, Y., Muralidharan, S., Murthy, C., Laventman, G.: Hyperledger fabric: a distributed operating system for permissioned blockchains (2018)